APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/800,561	03/15/2004	Shoichi Awai	7217/71978	9794

530   7590   08/08/2007
LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK
600 SOUTH AVENUE WEST
WESTFIELD, NJ 07090

EXAMINER
SANDERS, AARON J

ART UNIT	PAPER NUMBER
2168	

MAIL DATE	DELIVERY MODE
08/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

Office Action Summary	Application No. 10/800,561	Applicant(s) AWAI, SHOICHI
	Examiner Aaron Sanders	Art Unit 2168

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 June 2007*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-6* is/are pending in the application.

  4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-6* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 March 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

  Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

  Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

  a)☐ All   b)☐ Some * c)☐ None of:

  1.☐ Certified copies of the priority documents have been received.

  2.☐ Certified copies of the priority documents have been received in Application No. _____.

  3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

  * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114. Applicant's submission filed on 4 June 2007 has been entered.

Specification

The amendment filed 10 May 2007 is objected to under 35 U.S.C. 132(a) because it

introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall

introduce new matter into the disclosure of the invention. The added material which is not

supported by the original disclosure is as follows: "or a unique identification code assigned to

every AV server 30 by for example the manufacturer".

Applicant is required to cancel the new matter in the reply to this Office Action.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making
and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it
pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode
contemplated by the inventor of carrying out his invention.

Claim 1 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the

enablement requirement. The claim(s) contains subject matter which was not described in the

specification in such a way as to enable one skilled in the art to which it pertains, or with which

it is most nearly connected, to make and/or use the invention.

Specifically, it is not clear from the specification how an "optimum file size" is

detected/determined.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing

to particularly point out and distinctly claim the subject matter which applicant regards as the

invention.

The term "optimum" in claim 1 is a relative term which renders the claim indefinite. The

term "optimum" is not defined by the claim, the specification does not provide a standard for

ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably

apprised of the scope of the invention.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1 and 3-5 are rejected under 35 U.S.C. 102(e) as being anticipated by Yano et al.,

U.S. 6,711,594.

As per claims 1 and 3-5, Yano et al. teach:

1. A data service apparatus comprising:

storage means for storing digital data (See e.g. col. 2, lines 4-45, "a reading/writing

means for reading/writing digital data from/onto a portable recording medium");

an encryption circuit for encrypting digital data into encrypted data (See e.g. col. 2, lines

46-64, "a means for encrypting data");

a decryption circuit for decrypting encrypted data into its initial digital data (See e.g. col.

2, lines 46-64, "individual divided data are decrypted or, alternatively, to perform the decryption

after the divided data are integrated"), and

an identification code generation circuit for generating an identification code unique to

the data service apparatus (See e.g. col. 1, line 45 to col. 2, line 3, "a data management means for

recording... data-saving procedure information that indicates a dividing method of the data to be

saved and the like" which includes, see col. 6, lines 14-41, "A unique file name is designed to be

given to each of the divided files formed on the basis of the to-be-saved data file in accordance

with a predetermined rule"),

wherein digital data, to be backed up, stored in the storage means is extracted, encrypted

by the encryption circuit into encrypted data and stored in an external storage unit (See e.g. Fig.

3, S1 "medium reading and authentication", S23 "division/encryption", and S31 "divided file

writing" where, see col. 2, lines 4-45, "the divided parts are each transferred to the plurality of

servers on the network and are distributed/saved therein"); encrypted data, to be decrypted,

stored in the external storage unit is extracted, decrypted by the decryption circuit into the initial

digital data and written back to the storage means (See e.g. Fig. 3, S43 "reading of divided files

that constitute the to-be-extracted file", S47 "decryption/integration of divided files", and S51

"saving of the to-be-extracted file" where, see col. 2, lines 4-45, "it becomes possible to access

the saved data from an arbitrary distributed data archive device connected to the network as long

as the portable recording medium is carried with the user"); the encryption circuit is operable to

perform encryption by utilizing the identification code generated by the identification code

generation circuit (See e.g. col. 2, lines 46-64, "cryptographic key information and the like that

are needed for encryption/decryption are recorded as the data-saving procedure information by

the data management means" where, see col. 5, line 58 to col. 6, line 13, "For example, if the

data file F1 is divided into four divided files F11 to F14, these files F11 to F14 are distributed

and saved onto any one of the three data servers 2a to 2c of FIG. 1. In this case, information

about how the original data file F1 has been divided, about what bytes the size of each divided

file is, and about how many divided files have been formed in total is stored onto the

management folder of FIG. 2 as management data (data-saving procedure information) of the file

F1. If the encryption method, the redundancy storage method, the dummy data addition method,

etc., are employed at this time, information about these methods is also stored as management

data"); and the decryption circuit is operable to perform decryption by utilizing the identification

code generated by the identification code generation circuit (See e.g. col. 2, lines 46-64,

"cryptographic key information and the like that are needed for encryption/decryption are

recorded as the data-saving procedure information by the data management means" where, see

col. 6, lines 42-61, "Moreover, reference to data-saving procedure information in the

management data of the file F1 makes it possible to recognize a reconstituting procedure about

how the divided files that have been read should be decrypted"); and

a detection circuit for detecting an optimum file of digital data for storage as a file into

the external storage unit (See e.g. col. 10, lines 1-21, "Thereafter, the 'file division method' is

determined at step S13. In more detail, conditions are established about how the to-be-saved file

F1 is divided (i.e., algorithm), about how much file length the to-be-saved file F1 is divided to

have (i.e., file size), and how many files the to-be-saved file F1 is divided into (i.e., number of

files)... it is preferable that the conditions be automatically determined on the basis of a given

program prepared in the distributed data archive device 1. Preferably, the conditions depend on

each to-be-saved file, in order to improve security").

2. (Canceled)

3. The data service apparatus according to claim 1, further comprising a falsification

detection circuit for checking, when decrypting the digital data from the encrypted data, the

digital data according to the identification code generated by the identification code generation

circuit, and for inhibiting the initial digital data from being written back to the storage means

when it is found that the digital data has been falsified (See e.g. col. 13, lines 8-31, "Since an IC

card with very great security against illegal data falsification can be used as the archive card 10

needed when data is saved and when the data is extracted, there is no fear that saved data will be

stolen", col. 8, line 57 to col. 9, line 10, "The authenticity of the distributed data archive device

1... is checked on the side of the archive card 10 while the authenticity of the archive card 10 is

being checked by the verification means 12", and Fig. 3, S1 "medium reading and

authentication" where, if the data is falsified, it is not read).

4. The data service apparatus according to any one of claims 1and 3, further comprising a

comparison circuit for making a comparison in attribute data between the digital data in the

storage means and the digital data stored in the external storage unit (See e.g. col. 5, line 58 to

col. 6, line 13, "Information (i.e., URL list of the data servers) that shows the data server on

which each of the four divided files F11 to F14 is saved is stored onto the management folder of

FIG. 2 as management data (data depository information) of the file F1" where an attribute of the

data is the server's URL),

wherein digital data, which has been updated after being previously backed up in the

external storage unit and which is stored in the storage means, is stored into the external storage

unit depending upon a comparison result from the comparison circuit (See e.g. col. 4, lines 24-

52, "the data depository information is constructed by a list of addresses (i.e., Uniform Resource

Locator, which is hereinafter referred to as URL) of a plurality of data servers that are depository

destinations" where, see col. 13, lines 8-31, the data can be updated because "It is possible to

very conveniently access the saved data from an arbitrary distributed data archive device

connected to the network if the archive card 10 is carried").

5. The data service apparatus according to claim 4, further comprising:

an aggregation circuit for aggregating a plurality of files into one file (See e.g. col. 1, line

45 to col. 2, line 3, "an integration/reconstitution means for reconstituting divided/saved data into

an original single data file");

a division circuit for dividing a file into a plurality of files each having a predetermined

size (See e.g. col. 1, line 45 to col. 2, line 3, "a division means for dividing data to be saved into

a plurality of parts");

a synthesis circuit for combining the divided files together into one file (See e.g. col. 1, line 45 to col. 2, line 3, "an integration/reconstitution means for reconstituting divided/saved data into an original single data file"); and

a separation circuit for separating one file formed from a plurality files into the plurality of files (See e.g. col. 1, line 45 to col. 2, line 3, "a division means for dividing data to be saved into a plurality of parts"), wherein

for backup of the digital data:

digital data read by the aggregation circuit from the storage means are aggregated into one file (See e.g. col. 2, lines 4-45, "when the data to be saved is extracted, the data to be saved that has been distributed into the plurality of servers on the network and has been saved therein is extracted");

the file as a result of the aggregation is divided by the division circuit according to the size detected by the detection circuit (See e.g. col. 8, lines 19-32, "one divided file is constructed with data in which one byte is taken at every third byte if three divided files are formed"); and

the file as a result of the division being stored into the external storage unit (See e.g. col. 2, lines 4-45, "a network communication means for transferring the data files divided by a communication protocol determined among data servers keeping the data to be saved"); and wherein

for decryption of the digital data:

the encrypted data stored in the external storage unit are decrypted and combined by the synthesis circuit into an initial one file (See e.g. col. 2, lines 46-64, "the

integration/reconstitution means reconstitutes the divided data into the original data in such a

way as to perform the integration after the saved individual divided data are decrypted"); and

the file as a result of the synthetic combination is separated by the separation circuit into

the plurality of initial digital data and written back to the storage means (See e.g. Fig. 3, S51

"saving of the to-be-extracted file" where the file is saved to the card, Fig. 1 where there can be

more than one "to-be-saved data file", and therefore after the files have been individually

recombined from the data servers they are still separate from each other on the card and therefore

a "plurality of initial digital data and written back to the storage means").

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yano et al., U.S.

6,711,594, in view of Murty et al., U.S. 2003/0084290.

6. The apparatus according to claim 5, further comprising a communications circuit for

performing information communications with an external certificate server,

wherein restoration of the digital data to be decrypted is done only when the

communications circuit has received a permission of restoration from the external certificate

circuit (Yano et al. do not disclose using a certificate server to authenticate the access rights of

the portable storage medium. However, Murty et al. do make such a disclosure, see [0029], "To

obtain the symmetric storage key, the HSED 22 must authenticate itself with the security

appliance 20. This authentication may be achieved in any one of a number of different ways, but

preferably involves the HSED 22 sending a certificate signing request to the security appliance

20" where, see [0028], "the HSED 22 intercepts the incoming data and decrypts (using the

symmetric storage key 26) what is read from the drive before delivering this information to the

host server 12a". Yano et al. and Murty et al. are analogous art because they both discuss

protecting digital files transferred over a network. At the time of the invention, it would have

been obvious to one of ordinary skill in the networking art to combine the teachings of the cited

references because Murty's et al. teachings would have allowed Yano's et al. apparatus to use a

certificate server for authentication so as to gain "an improved post-side encryption module for

encrypting data for storage on a storage area network, and for decrypting encrypted data received

from the storage area network", see Murty et al. [0009], because "a security system for storage

area networks that provides certificate-based authentication, persistent encryption of data (during

movement and storage) and transparent operation (across all hardware and software components

found on the storage area network) is desirable", see Murty et al. [0008]).

Response to Arguments

As per Applicant's argument that Yano et al. do not disclose the limitation, "detecting an

optimum file size" in claim 1, the Examiner respectfully disagrees. While Yano et al. do not

explicitly use Applicant's terms, they do disclose the equivalent functionality. Specifically,

Applicant defines "detecting an optimum file size" as: "When the succession of files from the

aggregation circuit 33 is supplied to the division circuit 34 for storage into the external storage

unit 60, it is divided by the division circuit 34 into a plurality of files each having an optimum

size for that storage" (see the last paragraph beginning on pg. 6). The specification does not

mention a "detection circuit" nor does it define "optimum".

The Examiner has cited Fig. 1 where, see col. 10, lines 1-21, "Thereafter, the 'file

division method' is determined at step S13. In more detail, conditions are established about how

the to-be-saved file F1 is divided (i.e., algorithm), about how much file length the to-be-saved

file F1 is divided to have (i.e., file size), and how many files the to-be-saved file F1 is divided

into (i.e., number of files)... it is preferable that the conditions be automatically determined on

the basis of a given program prepared in the distributed data archive device 1. Preferably, the

conditions depend on each to-be-saved file, in order to improve security". Here, the

determination, i.e. the claimed detection, of an optimum file size is based on several

"conditions", e.g. "how the to-be-saved file F1 is divided", etc.

Conclusion

The prior art made of record and not relied upon is considered pertinent to Applicant's

disclosure: Takenaka et al., U.S. 5,917,908; Orsini et al., U.S. 2004/0049687; Satoh et al., U.S.

2004/0172538; and Lang et al., U.S. 2005/0005143.

Any inquiry concerning this communication or earlier communications from the

Examiner should be directed to Aaron J. Sanders whose telephone number is 571-270-1016. The

Examiner can normally be reached on M-Th 9:00a-5:00p.